REMARKS

A. GENERALLY

Applicant thanks examiners Ryan Jakovac and Karen Tang for extending the courtesy of a telephone interview to Applicant on April 2, 2009. Applicant's summary of the interview is attached hereto.

Claims 36-57 remain in the Application. Claims 1-17 were previously canceled. Claims 18-35 are canceled herewith. No new matter has been added.

B. CLAIM REJECTIONS

1. Claim Rejections Pursuant to 35 U.S.C. §103(a)

Claims 18, 19, 21, 23-26, 28 and 30-35 have been rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication 2007/0214083 filed by Jones et al. in view of U.S. Patent Application Publication 2001/0044818 filed by Liang (hereinafter, "Liang"). Claims 20 and 27 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Jones. Claims 22 and 29 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Jones in view of Liang and in further view of U.S. Patent Application Publication 2004/0006621 filed by Bellinson et al. (hereinafter, Bellinson).

New claim 36 recites the following limitations:

> 36. (New) A system for providing data filtering from a cable modem termination system (CMTS) in a cable data network comprising:
>
> the CMTS, wherein the CMTS comprises a packet counter, wherein the packet counter determines a number of packets sent to a subscriber device from the CMTS (herein, "downstream packets") and a number of packets originating from the subscriber device and sent to the CMTS (herein, "upstream packets"), and a data gateway agent;
>
> a datastore accessible to the data gateway agent for storing a data transfer rule selected by a subscriber, wherein the selected data transfer rule comprises filtering criteria selected by the subscriber, and
>
> wherein the gateway agent comprises instructions that cause the CMTS to:
>
> receive a packet prior to receipt of the packet by the packet counter;
>
> access the data transfer rule stored in the datastore;
>
> use the filtering criteria to determine whether the packet violates the data transfer rule;
>
> forward the packet to the packet counter for counting when the packet does not violate the data transfer rule;

> send the subscriber device a notification message when the packet violates the data transfer rule, wherein the notification message comprises a prompt to override the data transfer rule;
>
> receive a response from the subscriber device to the override prompt;
>
> discard the packet when the response to the override prompt is to not override the data transfer rule; and
>
> forward the packet to the packet counter for counting when the response to the override prompt is to override the data transfer rule.

Independent claim 36 is drawn to a system for providing data filtering at a CMTS.

Jones generally describes a system and method for providing prepaid data service. A subscriber pre-pays for services by creating a credit in an account. As the subscriber utilizes various services, the account is debited. When the account reaches a threshold, the subscriber's access to services is terminated, and the subscriber is directed to a website to add additional value to the account. A pre-paid account may be purchased for various services.

Liang describes a system and method for identifying and blocking unacceptable web content. The system comprises a proxy server connected between a client and the Internet that checks a requested URL against a block list that may include URLs identified by a web spider. If the URL is not on the block list, the proxy server requests the web content. When the web content is received, the proxy server evaluates the content for prohibited content. The proxy server may either block the retrieved web content or permit user access to it. The filtering of Liang operates on URLs or web content that is requested by a subscriber. Liang does not teach or suggest detecting a packet that is directed to a subscriber device outside of a session initiated by the subscriber.

Neither Jones nor Liang teaches sending a subscriber device a notification message when a packet violates a data transfer rule, prompting the subscriber to override the data transfer rule, discarding the packet when the subscriber elects not to override the data transfer rule, and forwarding the packet to a packet counter for counting when the subscriber elects to override the data transfer rule.

Based on the foregoing, claim 36 is patentable over the combination of Jones and Liang. Claims 37-46 as currently listed depend directly or indirectly from claim 36 and recite all of the limitations of that base claim. Claims 37-46 are, therefore, patentable over the combination of Jones and Liang.

Independent claim 47 recites limitations of similar scope to those discussed above with respect to claim 36. Based on the foregoing, claim 47 is also patentable over the combination of Jones and Liang. Claims 48-57 as currently listed depend from claim 47) and recite all of the limitations of that base claim. Claims 48-57 are, therefore, patentable over the combination of Jones and Liang.

C. SUPPORT FOR THE NEW CLAIMS

Independent claims 36 and 47 include limitations directed to the overriding of a determination that a packet violates a data transfer rule. New dependent claims 37-42 and 48-53 recite limitations directed to the criteria used to reject a packet.

The specification of the present application discloses these limitations at least in the following paragraphs (the following disclosures from the present application are illustrative and not to be considered limiting):

> [51] Data transfer filtering settings for some embodiments of the present invention can be grouped into: filtering rules based upon the Internet communication protocols; filter rules based upon data contents; and a few special filtering rule options.
>
> [84] When the CMTS receives an initiation packet as an upstream packet, an inside user is trying to make a connection from the CPE network to the Internet. Assuming that the packet contents are otherwise acceptable, the CMTS will allow the connection and create a cache entry that includes connection information such as IP addresses, TCP ports, sequence numbers, etc.
>
> [85] Subsequent packets received by the CMTS have their packet connection information extracted and compared to the cache. A packet is only allowed to pass through if it corresponds to a valid connection (that is, if it is a response to a connection which originated on the CPE network).
>
> [87] For example, hybrid stateful packet filtering may handle UDP packets in the following fashion. The filter creates an entry in a connection database when the first UDP packet is transmitted. A UDP packet from a less secure network (a response) will only be accepted if a corresponding entry is found in the connection table.
>
> [102] Preventing the transmission of personal information is often a high priority with cable data network subscribers. For example an application layer filter may block all data packets containing the telephone number, social security number, drivers' license, credit card number of the subscriber and subscriber's location. In the alternative, such information may be blocked for all but a subscriber with administrator login privileges.
>
> [106] Preferred embodiments of the gateway agent also allow data traffic to be limited to particular periods of time. Time based data blocking is even more preferably combined with other types of data filtering. For example, a parent may wish to restrict

instant messaging and online gaming to one hour per day while allowing unlimited access to educational Internet websites.

[113] Figure 7A and Figure 7B flowsheets illustrate how the data gateway agent responds upon detecting a data transfer rule violation 701. Comparing data packets against data transfer settings a violation is detected 701. Automatically a notification message is transmitted to the subscriber 710 and optionally logged 702. When logged, it is desirable to also log information permitting tracking of the source of the violation and other relevant diagnostic information.

[114] Data violations are initially separated into upstream data and downstream data 715. The subscriber is asked to allow data being sent 720 or received 730. If the data is not allowed, the data packets are discarded and the notification process ends 750.

D. CONCLUSION

Applicant respectfully submits that the claims as currently listed are in condition for allowance. Applicant requests that this response be entered and that the current rejections of the claims now pending in this application be withdrawn in view of the above amendments, remarks and arguments.

Respectfully submitted,

Elliott D. Light, J.D.
Registration No. 51,948
Jon L. Roberts, Ph.D., J.D.
Registration No. 31,293
MARBURY LAW GROUP, PLLC
11800 Sunrise Valley Drive, Suite 1000
Reston, VA 20191-5302
(703) 391-2900